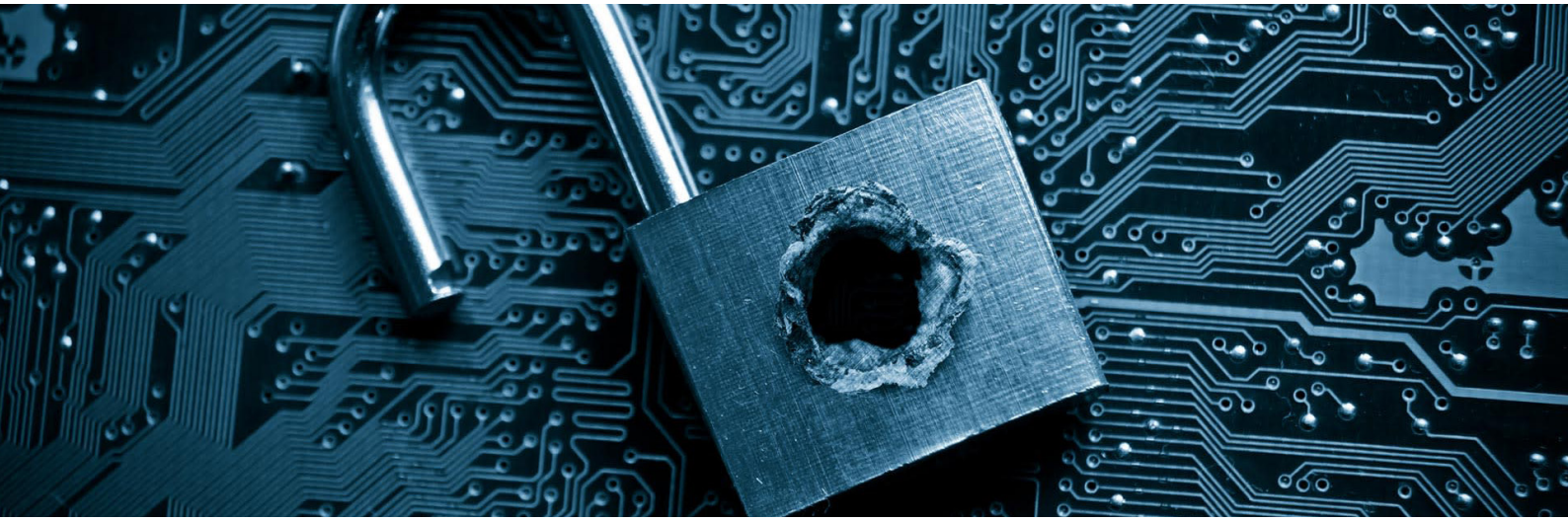
interlinked

NOTIFIABLE DATA BREACHES SCHEME

FACT SHEET: WHAT YOUR BUSINESS NEEDS TO KNOW



WHO IS AFFECTED BY THE NEW NOTIFIABLE DATA BREACHES (NDB) SCHEME?

Australia's Data Notification Law came into effect on February 22, 2018. It applies to businesses governed under the Privacy Act 1988 – including any with annual turnovers of $3 million, or businesses that collect and store sensitive user information like payment or personal data. If a data breach will likely result in "serious harm" to individuals, whether reputation, finances, or safety, you are required to notify the relevant parties. Failure to do so can incur fines of up to $1.8 million.

HOW BIG IS THE IMPACT?

According to the 2017 Cost of Data Breach Global Study by Ponemon Institute*, 1 in 4 organisations with top cyber security defences still experience data breaches. 90% of a cyber attack's bottom-line impact is felt up to two years after an attack. It is important to recognise that data breaches are not an "if" scenario, but "when". The new data breach laws add hefty fines and heightened public scrutiny on top of many other consequences of a breach, including: loss of sales and contracts, compromised IP, and legal action. Customers and shareholders will hold businesses responsible for non-compliance with these laws.

25% Organisations with top cyber security defences still experience data breaches

WHAT TO DO WHEN A BREACH IS DETECTED?

Verified breaches must be reported to the Australian Information Commissioner and all affected individuals, along with descriptions of the breach, the nature of any compromised information, and recommendations to individuals on what they should do next. The law gives organisations only 30 days to investigate any suspected breach, or plug any possible data loss, before notification is required.

HOW TO PROTECT AGAINST BREACHES?

Monitor your networks.

According to the Cost of Data Breach Global Study*, it takes an average of six months to discover a data breach. It's critical to have a robust monitoring system not only to help you and your team identify and stop threats more consistently, but also to make compliance with data breach notification laws much simpler. The more visibility you have into your data and networks, the easier it is to give details to regulators and the public if a breach occurs.

HAS A BREACH OCCURRED?

A notifiable data breach occurs when:

- Personal information is lost
- Personal information is disclosed to a third party
- A third party accesses personal information

THE NDB SCHEME APPLIES TO ANY BUSINESS WITH $3 MILLION ANNUAL TURNOVER OR COLLECTS & STORES SENSITIVE INFORMATION

WHAT AND WHEN TO REPORT?

- Publicly notify everyone whose personal information is involved
- Notify Office of the Australian Information Commissioner
- Make people aware and recommend response actions

YOUR BUSINESS HAS 30 DAYS TO NOTIFY OF THE BREACH

WHAT CAN YOUR BUSINESS DO NOW?

- Speak to your IT Department or Services Provider to organise a cyber security assessment
- Identify any potential vulnerabilities and pre-emptively design and implement security solutions

FAILURE TO NOTIFY CAN INCUR FINES OF UP TO $1.8 MILLION

QUESTIONS? ASK US.

1300 302 207
enquiries@interlinked.com.au

*2017 Cost of Data Breach Global Study by Ponemon Institute: https://www-03.ibm.com/security/au/en/data-breach